REMARKS

I. Introduction

Claims 30 to 59 are pending in the present application. In view of the foregoing amendments and the following remarks, it is respectfully submitted that all of the presently pending claims are allowable, and reconsideration is respectfully requested.

II. Rejection of Claims 30 to 38, 40 to 45, 47 to 52 and 54 to 58 Under 35 U.S.C. § 102(b)

Claims 30 to 38, 40 to 45, 47 to 52 and 54 to 58 were rejected under 35 U.S.C. § 102(b) as anticipated by European Published Patent Application No. 0 695 675 ("Hirozawa et al."). Applicant respectfully submits that claims 30 to 38, 40 to 45, 47 to 52 and 54 to 58 are patentable over Hirozawa et al. for at least the following reasons.

Claim 30 relates to a method for providing key verification for use with a security system, the security system including at least one valid key and an electronic verification arrangement having a transceiver for communicating with the at least one valid key, the electronic verification arrangement storing unique identification data for the at least one valid key and storing enable data corresponding to the unique identification data for the at least one valid key, the electronic verification arrangement generating an authority for accessing a secured object when authentication data is received from the at least one valid key. Claim 30 recites accessing the unique identification data for the at least one valid key in a mode of the security system. Claim 30 further recites performing a predetermined procedure to enter a key validation mode of the security system, the step of performing the predetermined procedure being performed by a user of the security system. Claim 30 further recites retaining enable data for each of the at least one valid key within a transceiver range in the key validation mode. Claim 30 further recites deleting other enable data for each of the at least one valid key outside the transceiver range in the key validation mode. Claim 30 as amended herein without prejudice recites that the method includes deactivating each of the at least one key for which the other enable data is deleted in the step of deleting to reduce a number of valid keys having enable data by a number of the valid keys outside the transceiver range in the key validation mode.

Claim 44 relates to a security system. Claim 44 recites that the security system includes at least one valid key and an electronic verification arrangement including a transceiver for communicating with the at least one valid key and including a mode for accessing unique identification data. Claim 44 as amended herein without prejudice recites that the electronic verification arrangement is operable to: store the unique identification data for the at least one valid key, generate an authority for accessing a secured object when authentication data is received from the at least one valid key, store enable data in accordance with the unique identification data for each activated one of the at least one valid key, enter a key validation mode when a user performs a predetermined procedure, retain enable data for each of the at least one valid key within a transceiver range in the key validation mode, and delete other enable data for each of the at least one valid key outside the transceiver range in the key validation mode to reduce a number of valid keys having enable data by a number of the valid keys outside the transceiver range in the key validation mode.

Claim 58 relates to a vehicle including a security system. Claim 58 recites that the security system includes at least one valid key and an electronic verification arrangement including a transceiver for communicating with the at least one valid key and including a mode for accessing unique identification data. Claim 58 recites that the electronic verification arrangement is operable to store the unique identification data for the at least one valid key, generate an authority for accessing a secured object when authentication data is received from the at least one valid key, store enable data in accordance with the unique identification data for each activated one of the at least one valid key, enter a key validation mode when a user performs a predetermined procedure, retain enable data for each of the at least one valid key within a transceiver range in the key validation mode, and delete other enable data for each of the at least one valid key outside the transceiver range in the key validation mode.

Hirozawa et al. purportedly relate to an anti-vehicle-thief apparatus and code setting method of the apparatus. The apparatus is stated to include, *inter alia*, a transponder 1 and an antenna 2 for receiving signals from the transponder 1. See col. 7, lines 48 to 51. The apparatus is stated to register specific ID codes of a plurality of keys and to determine validity of a key in accordance with an operation of the key including a transponder having one of the registered specific ID codes. The

apparatus is stated to register a code specific to the key or transponder and confirms an operation in which an ignition switch is turned on and off five times by using the key, where this operation is for changing the ID codes specific to the plurality of keys or transponders registered in EEPROMS. After the confirmation of the operation, ID codes specific to a plurality of new keys or transponders are stated to be successfully registered, thereby preventing a third person from using the old keys or transponders, as well as generating ID codes specific to the new keys or transponders. As part of the operation sequence of an additional write process in the immobilizer unit, all the ID codes except the ID code of the transponder which is under use are stated to be deleted. See col. 16, lines 19 to 20 and col. 14, lines 17 to 18. After the key in use is pulled out of the ignition another key is stated to be able to be placed in the ignition and its associated ID code registered in the immobilizer unit. See col. 14, lines 18 to 33.

Nowhere do Hirozawa et al. disclose, or even suggest, retaining enable data for each of the at least one valid key within a transceiver range in the key validation mode, deleting other enable data for each of the at least one valid key ***outside the transceiver range*** in the key validation mode, and deactivating each of the at least one key for which the other enable data is deleted in the step of deleting, as recited in claim 30. Further, nowhere do Hirozawa et al. disclose, or even suggest, retaining enable data for each of the at least one valid key within a transceiver range in the key validation mode and deleting other enable data for each of the at least one valid key ***outside the transceiver range*** in the key validation mode, as recited in claims 44 and 58. Firstly, Hirozawa et al. do not state that the key in the ignition is necessarily within a transceiver range. Rather, the sole qualification for ID code retention is that the key associated with the ID code be in the ignition. Further, Hirozawa is not selective as to which ID codes are deleted, i.e., with respect to deletion of ID codes, there is no distinction between keys based on their location or, more specifically, based on whether they are ***outside the transceiver range***, as recited in claims 30, 44 and 58. As indicated above, a key is placed in the ignition and the ID codes for all other keys, regardless of whether they are within the range of antenna 2, are deleted. See col. 16, lines 19 to 20 and col. 14, lines 17 to 18.

Claims 30, 44 and 58 recite a transceiver for communicating with the at least one valid key having a ***transceiver range***. In this regard p. 3, lines 13 to 17 of

the Specification states that "ECU 2 includes an rf transceiver 14 for generating an rf signal which excites the transponder of a remote key 4 of the security system when key 4 is within the vicinity of a vehicle." Hirozawa et al. do not disclose, or even suggest, the range of antenna 2 nor do they indicate whether the ignition switch is within the range of antenna 2. The Final Office Action states without any support that to "require placing of the key in the ignition is within the scope of the broadly claimed 'inside the transceiver range.'" Similarly, the Final Office Action states without any support that Applicant's alleged admission "that all other keys [in Hirozawa] are then deleted" reads on deleting data for keys not within the transceiver range. As indicated above, Hirozawa et al. do not disclose, or even suggest, the range of antenna 2 and make no distinction between keys inside and outside the range of antenna 2. Consistent with the disclosure of Hirozawa et al., assuming the range of antenna 2 extends beyond the ignition, keys outside of the ignition but within the range of antenna 2, for example, within the automobile cabin, are stated to be deleted, which is in direct contrast to the subject matter claimed. Therefore, Hirozawa et al. do not disclose all of the limitations of claim 30, 44 and 58.

Furthermore, as indicated above, claims 30 and 44 have been amended herein without prejudice to include the feature that the number of valid keys having enable data is reduced by a number of the valid keys outside the transceiver range in the key validation mode. Thus, valid keys that may have been lost, stolen or misplaced may be deactivated, without activating a corresponding number of lost, stolen or misplaced valid keys. According to Hirozawa et al., an equal number of keys are registered to the number of keys stolen or missing. See col. 13, line 54 to col. 15, line 8. That is, Hirozawa et al. do not disclose, or even suggests, reduction of a number of valid keys having enable data by a number of valid keys outside a transceiver range in a key validation mode. For this additional reason, it is respectfully submitted that Hirozawa et al. do not anticipate amended claims 30 and 44.

To anticipate a claim, each and every element as set forth in the claim must be found in a single prior art reference. Verdegaal Bros. v. Union Oil Co. of Calif., 814 F.2d 628, 631, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987). Furthermore, "[t]he identical invention must be shown in as complete detail as is contained in the . . . claim." Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 U.S.P.Q.2d

1913, 1920 (Fed. Cir. 1989). That is, the prior art must describe the elements arranged as required by the claims. In re Bond, 910 F.2d 831, 15 U.S.P.Q.2d 1566 (Fed. Cir. 1990). As more fully set forth above, it is respectfully submitted that Hirozawa et al. do not disclose, or even suggest, all of the limitations of claims 30, 44 and 58. It is therefore respectfully submitted that Hirozawa et al. do not anticipate claims 30, 44 and 58.

As for claims 31 to 38 and 40 to 43, which ultimately depend from claim 30 and therefore include all of the limitations of claim 30, Applicant submits that these claims are patentable over Hirozawa et al. for at least the reasons provided above in support of the patentability of claim 30.

As for claims 45, 47 to 52 and 54 to 57, which ultimately depend from claim 44 and therefore include all of the limitations of claim 44, Applicant submits that these claims are patentable over Hirozawa et al. for at least the reasons provided above in support of the patentability of claim 44.

In view of all of the foregoing, withdrawal of this rejection is respectfully requested.

III. Rejection of Claims 44 and 46 Under 35 U.S.C. § 102(b)

Claims 44 and 46 were rejected under 35 U.S.C. § 102(b) as anticipated by U.S. Patent No. 5,508,691 ("Castleman et al."). Applicant respectfully submits that claims 44 and 46 are patentable over Castleman for at least the following reasons.

Claim 46 depends from claim 44 and further recites that the predetermined procedure includes a vehicle entry procedure.

Castleman et al. purportedly relate to a self-contained electronic lock with changeable master and slave codes. The electronic lock is stated to include an erasable circuit including a nonvolatile memory for holding key codes in at least two memory locations. When all of the master key code memory locations are stated to be filled, a new key is stated to be programmable into the lock as a "slave key." See col. 10, lines 2 to 5. A particular slave key or all of the slave keys are stated to be deauthorizable. See col. 10, lines 50 and 63. Further, all of the keys, including the master key, are stated to be deauthorizable. See col. 10, line 1. The slave key is stated to be deauthorized by first touching the master key to the lock and then within 5 seconds touching the slave key to the lock. See col. 10, lines 51 to 62. All slave

keys are stated to be deauthorized by touching the master key to the lock twice within a five-second time period. See col. 10, lines 64 to 66. Key 20 is stated to be placed into electrical communication with RAM 12 of the microcontroller 10. See col. 8, lines 38 to 39. The electronics module 110 in the lock is stated to read a code number from a ROM in the key 120 through wires 122 and receptacle contacts on the key 120. See col. 6, lines 1 to 4.

Nowhere do Castleman et al. disclose, or even suggest, an electronic verification arrangement having a ***transceiver*** for communicating with the at least one valid key, as recited in claim 44. The Final Office Action alleges that element 21 qualifies as a transceiver. However, as indicated above, the electronics module 110 in the lock is stated to read a code number from a ROM in the key 120 ***through wires 122 and receptacle contacts*** on the key 120. See col. 6, lines 1 to 4.

Further, nowhere do Castleman et al. disclose, or even suggest, retaining enable data for each of the at least one valid key within a transceiver range in the key validation mode and deleting other enable data for each of the at least one valid key ***outside the transceiver range*** in the key validation mode, as recited in claim 44.

Castleman et al. do not discuss a transceiver or transceiver range, let alone selective retention and deletion of enable data based on distance from the transceiver, as recited in claim 44. As indicated above, slave keys, regardless of their location, are deauthorized by touching the lock in a certain manner with the master key. See col. 10, lines 51 to 62 and 64 to 66. Therefore, Castleman et al. do not disclose, or even suggest, all of the limitations of claim 44, and thus, do not anticipate claim 44.

As for claim 46, which ultimately depends from claim 44 and therefore includes all of the limitations of claim 44, Applicant submits that this claim is patentable over Castleman et al. for at least the reasons provided above in support of the patentability of claim 44.

In view of the foregoing, withdrawal of this rejection is respectfully requested.

IV. Rejection of Claims 39 and 53 Under 35 U.S.C. § 103(a)

Claims 39 and 53 were rejected under 35 U.S.C. § 103(a) as unpatentable over Hirozawa et al. Applicant respectfully submits that claims 39 and 53 are patentable over Hirozawa for the following reasons.

Claims 39 and 53 ultimately depend from claim 30 and 44, respectively, and further recite that the enable data includes a control byte.

As indicated above, Hirozawa et al. do not disclose, or even suggest, retaining enable data for each of the at least one valid key within a transceiver range in the key validation mode, deleting other enable data for each of the at least one valid key ***outside the transceiver range*** in the key validation mode, and deactivating each of the at least one key for which the other enable data is deleted in the step of deleting, as recited in claim 30. Further as indicated above, nowhere do Hirozawa et al. disclose, or even suggest, retaining enable data for each of the at least one valid key within a transceiver range in the key validation mode and deleting other enable data for each of the at least one valid key ***outside the transceiver range*** in the key validation mode, as recited in claim 44. Moreover, Hirozawa et al. do not disclose, or even suggest, reduction of a number of valid keys having enable data by a number of valid keys outside a transceiver range in a key validation mode Therefore, the Hirozawa et al. do not disclose all of the limitations of claims 39 and 53, which ultimately depend from claims 30 and 44, respectively.

The Final Office Action alleges that "[t]ransmission of enable data (control code) that has been encrypted by a numeric algorithm using the identification number as a seed when both sender and receiver know the seed is a typical in the industry and considered a 'safe' access procedure as the identification number is not sent and thus cannot be replicated." The Final Office Action further alleges that such "rolling code sequences are considered enabling data since only the key and transmitter know the next such 'enabling' code number" and that choosing "enable data to consist of only one byte (8 bits) rather than a smaller or larger number of bits would have been within the design choice of the security of the encrypting code." Applicant respectfully traverses these contentions to the extent that they are maintained and requests that the Examiner provide specific evidence to establish those assertions and/or contentions under 37 C.F.R. § 1.104(d)(2) or otherwise. In particular, it is respectfully requested that the Examiner provide an affidavit and/or that the Examiner provide published information concerning these

assertions. This is because this rejection is apparently being based on assertions that draw on facts within the personal knowledge of the Examiner, since no support was provided for these otherwise conclusory and unsupported assertions. (See also M.P.E.P. § 2144.03).

In rejecting a claim under 35 U.S.C. § 103(a), the Examiner bears the initial burden of presenting a prima facie case of obviousness. In re Rijckaert, 9 F.3d 1531, 1532, 28 U.S.P.Q.2d 1955, 1956 (Fed. Cir. 1993). To establish prima facie obviousness, three criteria must be satisfied. First, there must be some suggestion or motivation to modify or combine reference teachings. In re Fine, 837 F.2d 1071, 5 U.S.P.Q.2d 1596 (Fed. Cir. 1988). This teaching or suggestion to make the claimed combination must be found in the prior art and not based on the application disclosure. In re Vaeck, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991). Second, there must be a reasonable expectation of success. In re Merck & Co., Inc., 800 F.2d 1091, 231 U.S.P.Q. 375 (Fed. Cir. 1986). Third, the prior art reference(s) must teach or suggest all of the claim limitations. In re Royka, 490 F.2d 981, 180 U.S.P.Q. 580 (C.C.P.A. 1974). As stated above, Hirozawa et al. do not disclose, or even suggest, all of the limitations of claims 39 and 53. Therefore, Hirozawa et al. do not render claims 39 and 53 obvious. Therefore, withdrawal of this rejection is respectfully requested.

V. Conclusion

Applicant respectfully submits that all of the pending claims of the present application are now in condition for allowance. Prompt reconsideration and allowance of the present application are therefore earnestly solicited.

Respectfully submitted,

KENYON & KENYON

Dated: August 4, 2004 By: _____
Richard L. Mayer
Reg. No. 22,490

42,194

One Broadway
New York, New York 10004
(212) 425-7200
CUSTOMER NO. 26646